Synopsis of

On some techniques for Forgery Detection in Digital Images

A THESIS TO BE SUBMITTED FOR THE AWARD

OF THE DEGREE OF DOCTOR OF PHILOSOPHY

MODY UNIVERSITY OF SCIENCE AND TECHNOLOGY

Submitted By
Sunil Kumar
Enroll No. 090755

Prof. J. V. Desai
(Supervisor)

Prof. S. Mukherjee
(Co-Supervisor)

NOVEMBER, 2014

MODY UNIVERSITY OF SCIENCE AND TECHNOLOGY

(Formerly Mody Institute of Technology and Science)

FACULTY OF ENGINEERING & TECHNOLOGY

LAKSHMANGARH, SIKAR-332311

Contents

1. **Introduction**
2. **Motivation**
3. **Literature Survey**
4. **Research Work**
   - 4.1 A fast block based method for copy move forgery detection
     - 4.1.1 Proposed work
     - 4.1.2 Experimental results
     - 4.1.3 Conclusion
   - 4.2 Intensity invariant method using DCT-PCA transforms
     - 4.2.1 Proposed work
     - 4.2.2 Experimental results
     - 4.2.3 Conclusion
   - 4.3 Contrast invariant method using binary DCT vectors
     - 4.3.1 Proposed work
     - 4.3.2 Experimental results
     - 4.3.3 Conclusion
   - 4.4 A fast key point based hybrid method for copy move forgery detection
     - 4.4.1 Proposed work
     - 4.4.2 Experimental results
     - 4.4.3 Conclusion
   - 4.5 ICA based method to detect forgery
     - 4.5.1 Proposed work
     - 4.5.2 Experimental results
     - 4.5.3 Conclusion
5. **List of Publications**
6. **References**

1. Introduction

Images are a major source of information exchange in the digital world. Digital images are used to illustrate facts, establish facts and used by the newspapers to strengthen the stories published. Also digital images are used as corroborative evidences in criminal investigation. So it is very much necessary to ensure the truth of what is being believed. The issue of forged images is not new, but with the advancement of technology, it has become easier to manipulate an original image either to mislead the audience or to form a particular public perspective about famous personalities. Many instances [1] have been reported in the past to justify the claim. Digital image forgery detection has been growing very fast in the recent years as research domain [2].Broadly the forgery techniques can be classified in to copy move forgery or cloning, splicing and retouching [3] . Retouching is done to make minor changes in images by applying different filters as shown in figure 1. In splicing some part of intended image is replaced by the content from some other image as shown in figure 2. So the statistical parameters of that region are quite different from rest of the image. Statistical techniques are applied to detect such forgeries. However in copy move forgery same image content is used to hide some region of the same image as shown in figure 3.

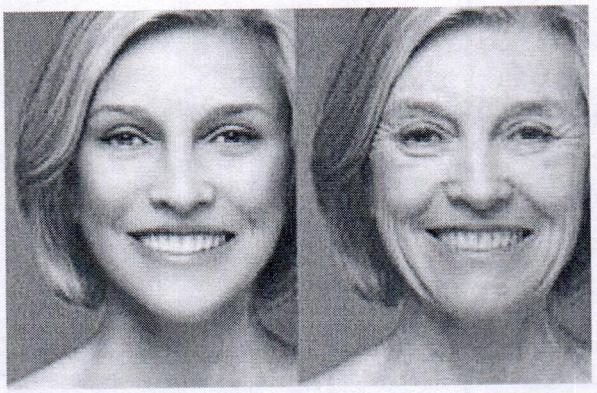


Figure.1 (Image retouching)

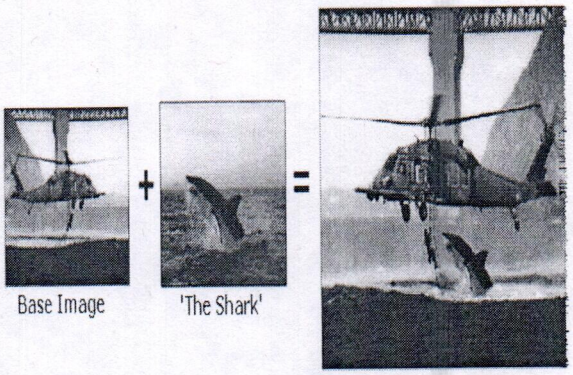


Figure.2 (Image splicing)

Figure.3 (Copy Move forgery: forged image on the left and original image on the right)

Forgery detection techniques can be classified into two broad categories [4]; active and passive or blind. In active techniques some prior knowledge is used about the original image to detect the tampering in the presented image. One example of such technique is digital watermarks [5] .In passive or blind techniques there is no prior information available about the original image. Copy move forgery detection using blind methods has picked up as hot research topic due to its wide veracity and applicability. The very fact about natural images that no significant regions are exactly same in an image is exploited in all such techniques. So if there is a sizable region to hint duplication then that is treated as case of copy move forgery. The commonly used approach in all pixel based methods [6] is shown in figure 4. In the preprocessing step the colored image is converted in to grayscale image by merging red, green and blue channels. After getting gray scale image either it is divided into blocks or key points are extracted. In block based approaches the input image is divided into overlapping blocks and feature vectors are extracted for each block. The resultant feature vectors are sorted and matched to find similar vectors. In an alternate approach some keypoints are extracted and feature are calculated only at these points to reduce the number of features to be compared.

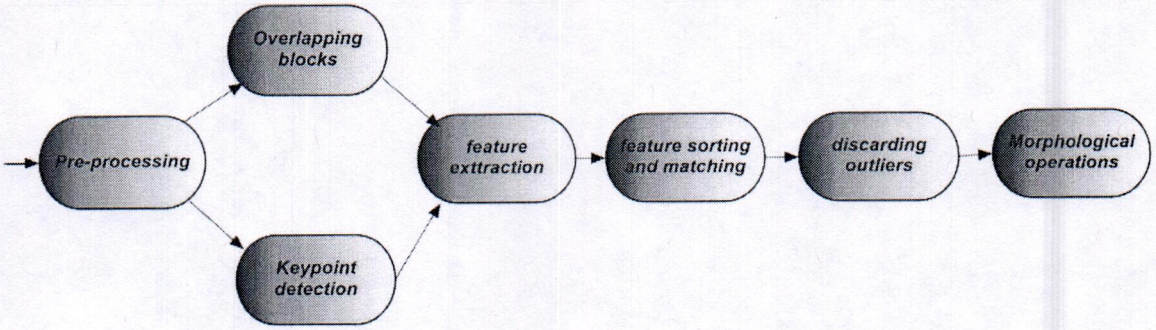


Figure 4. (Copy move forgery detection flow)

Different transform techniques like DCT, PCA, DWT, FMT etc. are used to convert the pixel data into more efficient and robust feature vectors. A summary is given in table 1 below.

Table 1
Grouping of feature sets for copy move forgery detection

Group	Features
Moment based	BLUR[7]
	ZERNIKE[8]
Dimensionality reduction	PCA[9]
	SVD[10]
Frequency	DCT[11]
	DWT[12]
	FMT[13]
Key point	SIFT[14]
	SURF[15]

2. Motivation

Although many techniques have been suggested by researchers, there are many issues in such techniques like the detection time, feature collection from the blocks, and matching techniques to efficiently find similar blocks/keypoints. Also to make it difficult for forgery detection, the manipulator performs some post copy-paste operations like adding some noise, compressing the manipulated image, rotation, scaling and change of illumination like intensity and contrast. So there is ample scope for improvement in all the above stated parameters and hence obviously enhancing the overall performance in the forgery detection process. In recent times one can see significant rise in the research on copy move forgery detection and hence making it an interesting and significant research domain.

3. Literature Survey

The first block based method was proposed by Fridrich et al. [11] based on discrete cosine transform (DCT). Popescu and Farid [9] altered the block representation and instead of DCT used principal component analysis (PCA). Huang et al [16] suggested an improved method using DCT coefficients. Luo et al [17] divided blocks into four sub-blocks, which were evaluated according to an average of red, blue and green color values. This method proved robust to attacks, such as JPEG compression, Gaussian blurring, and additive noise. An approach using combination of DWT and DCT is suggested in [12]. Discrete wavelet transform is used to reduce the size of image and then DCT is applied on low frequency component achieved by DWT. Singular value decomposition (SVD) is applied to each image block to yield a representation with reduced dimensions in [10]. This approach proved robust against noise distortion and more efficient. DCT blocks are converted into circular blocks and divided into four regions to get feature vectors in [18]. Local binary patterns are used to get the binary feature vector for robust and efficient matching in [19] [20]. Bayram et al. [13] applied a Fourier Mellin transform (FMT) and 1-D projection of log-polar values in a robust scheme for the detection of image forgeries. Lynch et al. [21] proposed an efficient expanding block algorithm based on direct block comparison rather than indirect comparisons based on block features. Local interest points (e.g. SIFT and SURF) have been widely used for image retrieval and object recognition, due to their robustness in dealing with numerous geometrical transformations (such as rotation and scaling) and occlusions. Recently, attempts have been made to apply these types of features in digital forensics. Keypoint based methods differ from block-based methods in their reliance on the identification and selection of regions of high-entropy within an image (i.e. "keypoints"). Scale-invariant feature transform (SIFT) is used in [22][14], which is capable of detecting and describing clusters of points belonging to cloned areas. Amerini et al. [23] developed a SIFT-based method for the detection of copy-move attacks and transformation recovery. Another keypoint based method using speeded up robust features (SURF) is used in [15] which is faster than SIFT. Jaberi et al [24] used SIFT like feature MIFT to claim higher robustness. However the all keypoint based methods are having limitations of key point extraction as keypoints from specific locations only can be extracted. Moreover, copied region with little textural structure may be missed entirely. So both approaches have their strengths and limitations.

4. Research work

The research work undertaken is divided into three sections. In Section 4.1-4.3 block based technique is used to address challenges in copy move forgery detection like time complexity and post processing operations of changing intensity and contrast. Section 4.4 deals with post processing operations like rotation and scaling using keypoint based method. Section 4.5 explores the blind source separation method using Independent Component Analysis (ICA). All the methods are tested on images taken from two datasets [25] and [26] . Also some images are captured with personal camera. There are total 200 images taken for each experiment in which 20 original images are taken and rest are forged. The methods are tested for robustness against common post processing parameters like noise, JPEG compression ratio etc. Further for testing robustness of the algorithm zero mean Gaussian noise is added to the forged images ranging from SNR 90db to 20db. Also some images are compressed using JPEG compression with compression ratio up to 40%. The algorithms are coded in MATLAB 2013a on a machine equipped with Intel i5 2.5 GHz processor with 8GB DDR3RAM.

4.1 A fast block based method for copy move forgery detection

4.1.1 Proposed Work

The proposed method uses block based method. For extracting feature vectors Discrete Cosine Transform is used. The DCT coefficients can be calculated as follows:

$$D(u,v)=\frac{2}{b}C(u)C(v)\sum_{x=0}^{b-1}\sum_{y=0}^{b-1}I(x,y)\cos\left(\frac{\pi u(2x+1)}{2b}\right)\cos\left(\frac{\pi v(2y+1)}{2b}\right)$$

Where

$$C(u)=\begin{cases}\frac{1}{\sqrt{2}} & if\ u=0\\ 1 & otherwise\end{cases}$$

$C(v)$ is similar to $C(u)$.

$D(u,v)$ are DCT coefficients for image I over block size b. DCT coefficients have very nice energy compaction characteristics. The first coefficient represents the average intensity over the block and termed as DC coefficient. High frequency DCT coefficient represent minor variations over the DC coefficient. This property is exploited in the proposed method to improve the existing DCT based method[11]. Only the feature vectors for which the DC components fall in a range are further processed reducing the amount of feature vectors to be

processed for next stage. The proposed method uses the DCT coefficients to represent the overlapping block. The DCT coefficients are ordered in zigzag manner to keep the low frequency coefficients together and before the high frequency coefficients in the row vector. The proposed algorithm works as follows:

(1) The input image is a gray scale image 'I' of the size m x n. If it is a color image, it can be converted to a grayscale image using the standard formula, $I = 0.299R + 0.587G + 0.114B$. R, G, B represents the three color components of RGB color model.

(2) Slide a fixed-sized b x b square window by one pixel from the upper left corner to the bottom right of the image 'I' to divide it into $(m-b+1)(n-b+1)$ overlapping blocks.

(3) Apply DCT to every block and reshape the b x b quantized coefficient matrix to a row vector by ordering DCT coefficients in zigzag order. To reduce the size of the vector and to retain only low frequency coefficients, the vector is truncated to only p x b^2 elements to retain only low frequency coefficients. The parameter 'p' is for deciding the number of coefficients retained.

(4) All vectors are sorted lexicographically and form a $(m-b+1)(n-b+1) \times pb^2$ matrix 'A'.

(5) For each row a_i in 'A', test its neighboring rows a_j which satisfy the condition that the first 'q' quantized DCT coefficients are same. As these DCT coefficients are sufficient to represent the major intensity distribution over the block.

(6) If a_i and a_j come out to be similar, the distance between two should be more than the block size i.e. 'b'.

(7) If distance between similar blocks is greater than' b', then calculate the shift vector 's' and increase the count for's'.
Where $s = (s_1, s_2) = (i_1-j_1, i_2-j_2)$ where similar block coordinates are (i_1, j_1) and (i_2, j_2).

(8) The highest count of's' is taken to be threshold frequency. Also, it should be more than b x b to represent some significant duplication.

(9) For all the blocks having shift value greater than the threshold value, mark the regions in the image with red color to represent copy moved regions.

4.1.2 Experimental results

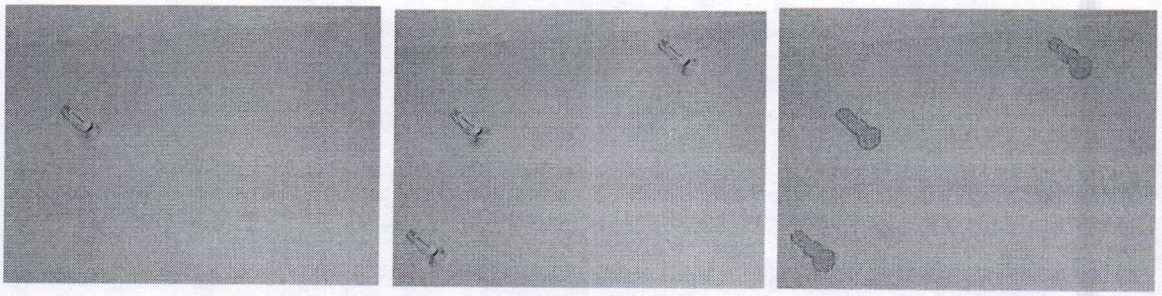


Figure 5. Low contrast image (standard deviation=0.0367). Left: Original image of a bulb on the wall, middle: forged image with the bulb region duplicated at two places, right: result of the proposed method showing the similar regions in red color.

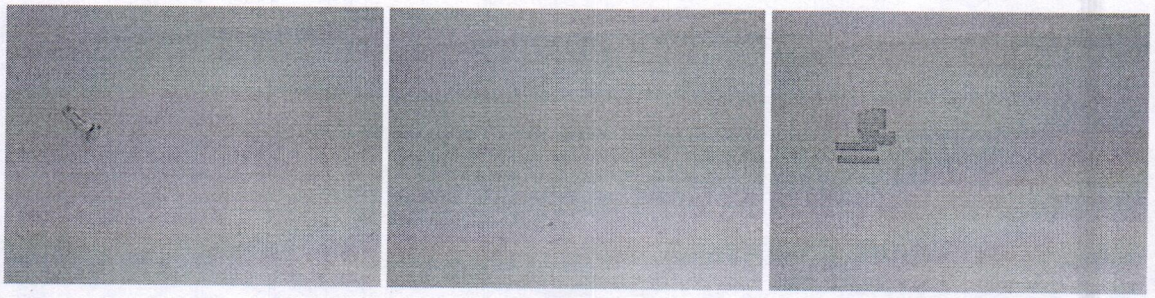


Figure 6. Low contrast image (standard deviation=0.0367). Left: Original image of a bulb on the wall, middle: forged image with the bulb region is hidden using multiple surrounding regions and blurred edges, right: result of the proposed method showing the similar regions in red color.

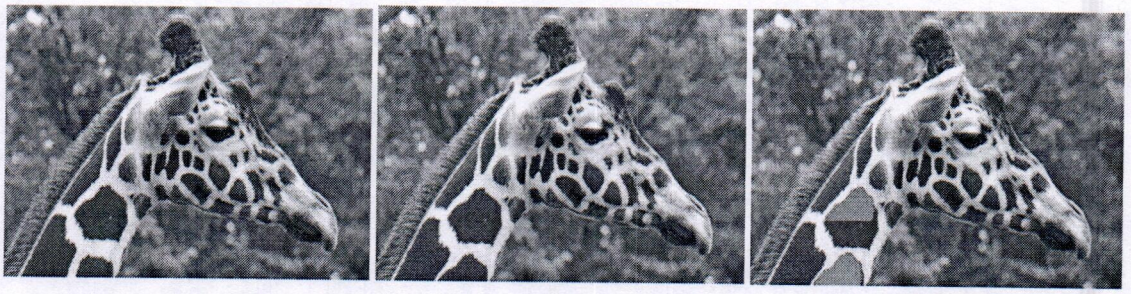


Figure 7. High resolution image (800x533). Left: Original image of a giraffe, middle: forged image with small portion of the pattern duplicated, right: result of the proposed method showing the similar regions in red color.

4.1.3 Performance Evaluation

The success rate of algorithm against post processing operations is measured as per below equation.

$$Success\ Rate = \frac{T_P}{T_P + F_P + F_N}$$

Where T_P is number of images correctly categorized as forged and F_P are the number of images falsely categorized forged and F_N are the number of forged images where forgery could not be established. The number of images for measuring the success rate in presence of post processing operations of added noise, JPEG compression, scaling and rotation is 50 each.

TABLE-2 PERFORMANCE COMPARISION

Image name/Image size	***Block size***	**Execution Time in Seconds**		**Number of potentially similar blocks**	
		Existing method[11]	***Proposed method***	***Existing method***[11]	***Proposed method***
bulb.bmp (640x480)	4x4	23.34	14.47	870409	12796
	8x8	25.24	17.8	848976	4685
	16x16	33.20	25.10	821736	1560
wall.bmp (640x480)	4x4	23.68	14.23	869631	9730
	8x8	24.69	16.47	847532	1697
card.bmp (640x480)	4x4	23.35	14.19	846302	2569
	8x8	25.88	16.24	826650	984
park.bmp (256x256)	4x4	4.95	3.5	183492	5391
	8x8	5.32	3.92	174812	4664
	16x16	6.4	5.43	158623	3469
giraffe.bmp (800x533)	4x4	31.66	19.55	1252903	9702
	8x8	36.03	22.43	1236590	3455
	16x16	46.94	34.62	1203396	2243

4.1.4 Conclusion

The proposed method has resulted in improving the detection speed and successfully automated threshold values which are set manually in the existing methods. Also the method retains the robustness against noise addition, JPEG compression, small rotations and scaling. Hence contributing a significant method. The proposed method detected forgery with 100% success rate for a given SNR above 50db. The success rate comes down to 90% for SNR below 40db. It significantly drops to 50% for the SNR values below 40db.The results are also checked for robustness against JPEG compression and 100% success rate is observed up to quality factor 8.The success rate falls down to 50% for JPEG quality factor 7.5.The proposed algorithm is robust against minor scaling and rotation up to 2%.

4.2 Intensity invariant method using DCT-PCA transforms

4.2.1 Proposed work

The proposed method addresses a particular type of robustness against change of intensity of the copy moved region. The manipulator may increase or decrease the brightness of the copy moved region to fit in some other part of the image. In such cases the DC component of the DCT feature vector will be significantly different even for the copy moved regions and evade the existing DCT based forgery detection techniques. However other components in the feature vector will be same. So the low frequency coefficients have been down sampled using very large quantization factor. The updated feature vector is invariant to the intensity variations of the copy moved part. However, it is assumed that the intensity variation will be uniform at least over the single block. It has been proved that PCA can be used directly in DCT domain [27]. So PCA is applied to reduce the dimensionality of the feature vector. To further reduce the time taken by the algorithm DCT coefficients are calculated in parallel for the overlapping blocks. Also to make the detection process more efficient, morphological operations are used to remove the isolated pixels and only retain the significant connected components. The algorithm structure is as follows:

(1) The input image is a gray scale image I of the size m x n. If it is a color image, it can be converted to a grayscale image using the standard formula I = 0.299R + 0.587G + 0.114B.

(2) A fixed-sized b x b window is slided one pixel along from the upper left corner to the button right, dividing I into (m-b +1)(n-b +1) blocks.

(3) For each block, apply DCT and reshape the b x b coefficient matrix to a row vector in zigzag order.

(4) Down sample the low frequency coefficients by using large quantization factor such that the DC component is very close to zero.

(5) Do PCA to the array of row vector to reduce the dimensionality and result a m-b +1)(n-b +1) x qb^2 matrix A.

(6) Use lexicographical sorting on A to sort the row vectors according to their similarity.

(7) For each row a_i in A, test its neighboring rows a_j which satisfy the threshold condition of minimum distance between duplicated rows (N_n).

(8) If the distance between similar blocks (N_d) is greater than block size, then a shift vector 's' is calculated and normalized.

$s= (s_1, s_2) = (i_1-j_1, i_2-j_2)$, where (i_1, j_1) and (i_2, j_2) are similar block coordinates . Then the shift vector's existing frequency is increased by one.

(9) The frequency matrix is sorted and third value is taken to be threshold frequency (N_f). Also it should be more than b x b.

(10) For all the blocks having shift value greater than the threshold mark (N_f) the block points in the dark image are registered as white points.

(11) Finally apply morphological operations to remove the isolated points and show the binary image as output representing copy moves regions with white regions.

4.2.2 Experimental results

The output of the proposed method for selected images is shown below. The intensity of the copied part is varied using Adobe Photoshop on a scale of 100.

Fig. 8. (a) Original image barrier.bmp.

Fig. 8. (b) Tampered image with intensity variation of (+10) in copy moved region.

Fig. 8. (c) Detection result of proposed method.

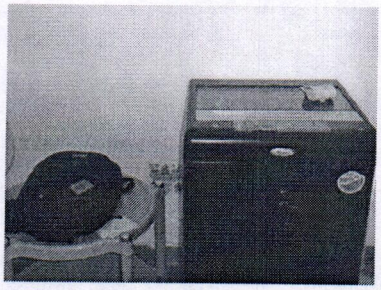


Fig. 9. (a) Original image logo.bmp.

Fig. 9. (b) Tampered image with intensity variation of (+80) in copy moved region.

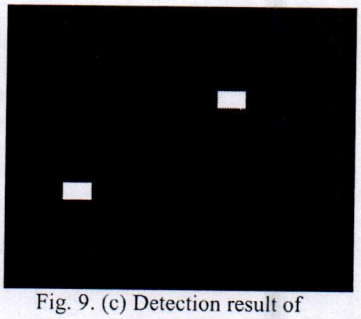


Fig. 9. (c) Detection result of proposed method.

Fig. 10. (a) Original image cap.bmp.

Fig. 10. (b) Tampered image with intensity variation of (-50) in copy moved region.

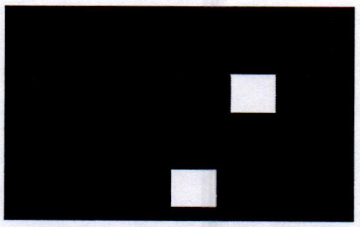


Fig. 10. (c) Detection result of proposed method.

TAB LE-3 PERFORMANCE COMPARISION OF THE PROPOSED METHOD WITH EXISTING METHODS

Image name/Image size	Intensity variation in the copy moved part	Block size	Copy Move attack detected successfully		
			Method in [9]	Method in [11]	Proposed method
barrier.bmp (800x600)	0	8x8	yes	yes	yes
	+10	8x8	no	no	no
	+10	4x4	no	no	yes
logo.bmp (640x480)	+50	8x8	no	no	yes
	+80	8x8	no	no	yes
	-10	8x8	no	no	yes
cap.bmp (640x480)	-50	8x8	no	no	yes
	+20	8x8	no	no	yes
pen.bmp (640x480)	-2	8x8	no	no	yes

4.2.3 Conclusion

Figure 8-10 show the visual results of the proposed algorithm on some selected images from the dataset. Table 3 provides comparative analysis. The method in [11] and [9] fails to detect the manipulation even with slight change in the intensity of the copy moved region. The default block size of 8x8 detects forgery successfully with an accuracy of 95%. However when the copy moved region is significantly smaller than 8x8, then the block size has to be changed to 4x4 as shown in Figure 8. The proposed method is successful in detecting the copy moved region with the changes in the intensity. Also PCA has been used for dimensionality reduction in DCT domain and the method retains the robustness against noise, JPEG compression and small amount of rotation and scaling.

4.3 Contrast invariant method using binary DCT vectors

4.3.1 Proposed work

This method extends the utility of DCT coefficients to achieve robustness against contrast changes. To make the row vectors contrast invariant we have proposed a binary form of DCT vector. It has been observed that the signs of the DCT coefficients do not change by the change of contrast of image upto certain level. This property has been exploited in the present work to make the forgery detection method invariant to any change in the contrast. The row vector is converted into binary vector by the following formula:
If a row vector of DCT coefficients is represented as

$$r_m = c_{m0}, c_{m1}, c_{m2}, c_{m3} \dots \dots \dots \dots c_{m,n}$$

Then DCT coefficient c_{mn} is modified as follows:

$$c'_{mn} = \begin{cases} 1 & if\, c_{mn} > 0 \\ 0 & else \end{cases}$$

After applying this operation the resultant row vectors are simply binary vectors. For matching the near duplicate regions, corresponding feature vectors must be matches. Three techniques have been tried namely Euclidean distance, Hamming distance and coefficient of correlation. The later has worked best in the proposed method. Coefficient of correlation between two binary vectors

$$r_m = c'_{m0}, c'_{m1}, c'_{m2}, c'_{m3} \dots \dots \dots \dots c'_{m,n} \text{ and}$$
$$r_{m'} = c'_{m'0}, c'_{m'1}, c'_{m'2}, c'_{m'3} \dots \dots \dots \dots c'_{m',n}$$

is calculated as follows:

$$\rho(r_m, r_{m'}) = \frac{cov(r_m, r_{m'})}{\sqrt{cov(r_m, r_m) cov(r_{m'}, r_{m'})}}$$

4.3.2 Performance evaluation

The performance of the method is evaluated according to following criteria:

$$D_c = \frac{p(I) \cap p(I') + q(I) \cap q(I')}{p(I) + q(I)}$$

$$D_f = \frac{p(I) - p(I') + q(I) - q(I')}{p(I') + q(I')}$$

where D_c, D_f are the correct detection ratio and false detection ratio respectively. I and I' are the given image and the output image after applying the forgery detection algorithm. $p(I)$ represents the number of pixels covered by the original area in image I. $q(I)$ represents the number of pixels in the forged region in the given image$I$. Intersection represents the common areas detected correctly. Difference represents the falsely identified pixels either original or

forged. So the D_c represents the precision with which the algorithm detects the forged areas. Larger D_c is better. D_f represents imprecision, hence lower is better. D_c , D_f are measure of stability of the method. Also the ability to detect the forged area correctly is represented by e i.e. efficiency.

$$e = \frac{q(I) \cap q(I')}{q(I)}$$

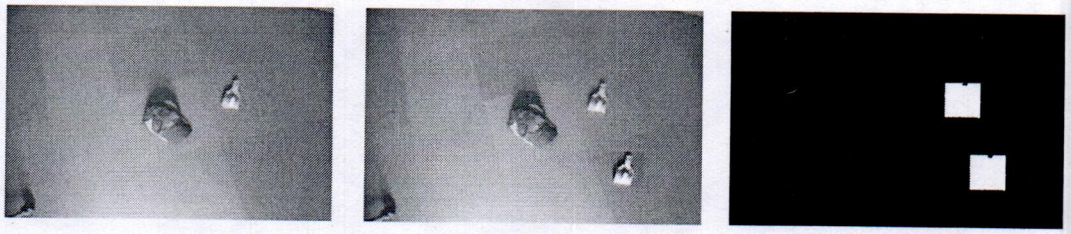
4.3.3 Experimental results

The experiment is conducted for block size=4. Contrast values are changed using Adobe Photoshop on a scale of 100.

Table -4 Comparison of efficiency of the proposed method with the existing methods

Contrast range (local)	DCT[11]	PCA[9]	Improved DCT[16]	Proposed
-25 to -20	0.00	0.00	0.00	0.87
-20 to -15	0.00	0.00	0.05	0.90
-15 to -10	0.12	0.00	0.32	0.92
-10 to -5	0.32	0.02	0.41	0.93
-5 to 0	0.51	0.21	0.52	0.95
0 to +5	0.42	0.22	0.46	0.95
+5 to +10	0.32	0.05	0.41	0.94
+10 to +15	0.11	0.00	0.21	0.93
+15 to +20	0.00	0.00	0.00	0.92
+20 to +25	0.00	0.00	0.00	0.90

The results in table-4 shows that the proposed method is very stable and works with reasonably good efficiency. The proposed method detect forgery efficiently up to 80% JPEG compression ratio. The method is also quite robust against noise and works efficiently up to SNR value 60.



(a) (b) (c)

Figure 11. Result of forgery detection in the presence of local contrast variation of +20.

4.3.3 Conclusion

The proposed method outperforms the existing compared methods in terms of the detection area efficiency. Also the length of the feature vector used in the proposed method is only 4, which is lesser than the compared methods. It is observed that in extreme contrast changes the efficiency is slightly more in case of positive contrast.

4.4 A fast key point based hybrid method for copy move forgery detection

Key point based methods have been used to detect image forgery in large size images, where block based techniques takes quite longer to detect forged regions. A hybrid approach is used in the proposed method by using different keypoint detector and descriptor.

4.4.1 Proposed work

Key points in a digital images are distinguishable pixel locations either due to unique intensity distribution around them or their invariance to affine operations. There are three major steps in a method using keypoints.

(i) Key point detection

(ii) Key point descriptors

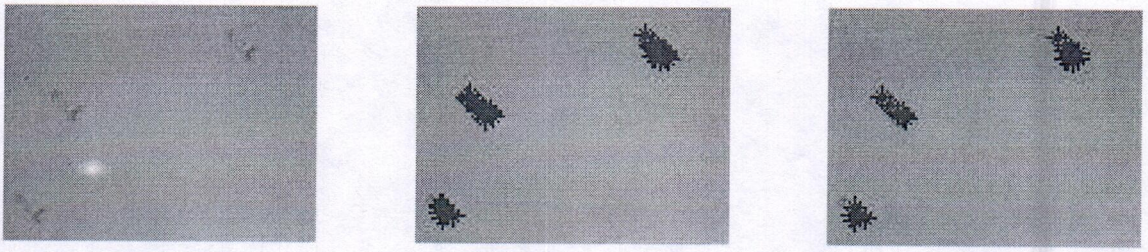
(iii) Identifying similar key point descriptor

In the proposed method different techniques are used for detection and description phase. SURF[28] is used to detect the potential key points in a given image and then BRISK[29] descriptors are generated using those key points. The time taken to generate BRISK descriptors is considerably less than SURF. The effectiveness of the method is tested on wide range of images for its Robustness against rotation, scaling, and Gaussian noise and JPEG compression ratio. As BRISK descriptors are binary descriptors. Matching process is also faster. Hamming distance is used as the criterion for finding the potential neighbors. *Knn*

search is applied for finding neighbors with k=3. Also a threshold value (ρ) is used to discard outliers. A keypoint is outlier if $(d_{ij}/d_{ik})>\rho$, where d_{ij} and d_{ik} are hamming distances of immediate neighbors of i^{th} feature.

4.4.2 Experimental Results

The method uses matching features keypoint locations to show copy moved area. Results on some selected images are shown.



Left: forged image

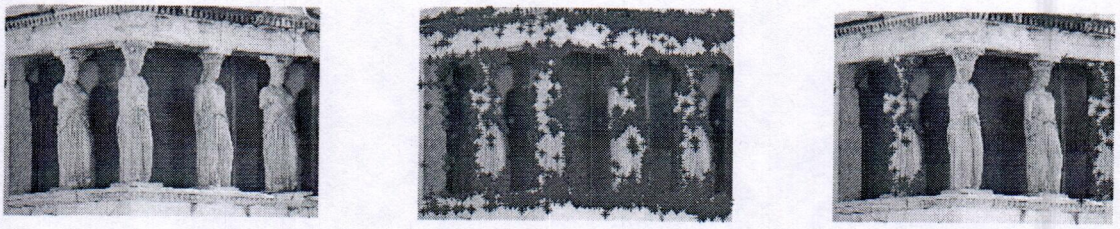
Figure 12.
Middle: keypoints generated

Right: final result

Left forged image

Figure 13.
Middle: keypoints generated

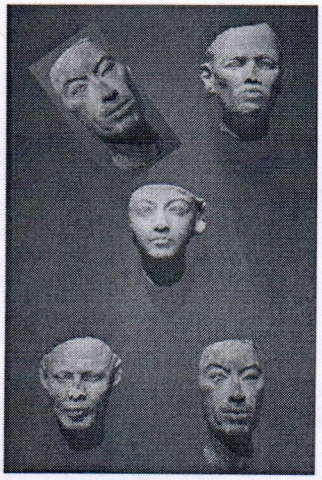
Right: final result



Left forged image

Figure 14.
Middle: keypoints generated

Right: final result



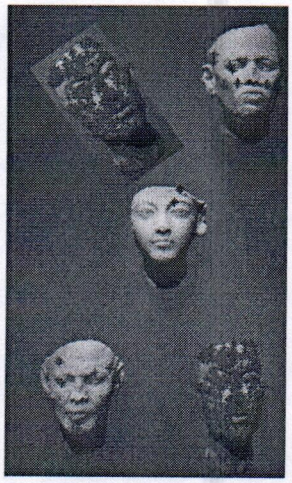


Figure 15.
Left forged image Middle: keypoints generated Right: final result

Figure 12 shows the result in the presence of low contrast and noise (SNR=40db). Figure 13 shows the results with copy move operation with rotation of 2 degrees. Figure 14 shows result of the method in the presence of JPEG compression ratio 70%. Figure 15 shows output of the method in presence of combination of scaling (107% both horizontal and vertical) and rotation of 35 degrees.

TABLE 5. COMPARISION OF DETECTION TIME WITH EXISTING SURF BASED METHOD

Forged image name	***Image size in pixels***	**Detection Time in Sec.**	
		Existing method [23]	***Proposed method***
bullb_n_40.bmp	480×640	0.56	0.18
horses_copy_r8_gcs500.png	1007×1520	0.8	0.54
egyptian_copy_r2_gcs500.png	1007×1520	1.07	0.80
lone_cat_copy_r2_gcs500.jpg	1007×1520	1.38	1.07
writing_history_copy_r10_gcs500.png	1007×1520	1.47	0.90
hedge_copy_r10_gcs500.png	1224×1632	0.61	0.31
sails_copy_r2_gcs500.png	1296×1944	1.73	1.3

Forged image name	*Image size in pixels*	Detection Time in Sec.	
		Existing method [23]	*Proposed method*
kore.bmp	2592×3872	4.38	3.01
maskcopy.bmp	3039×2014	1.67	0.81
mask_r35_s107 .bmp	3039×2014	1.72	1.36

4.4.3 Conclusion

The proposed method is quite robust to the commonly applied post processing operations of rotation and scaling. The method is able to locate copy move forgery even for large values of rotations and scaling. Also BRISK descriptors calculation is faster than the SURF descriptors and hence there is significant improvement in the detection speed.

4.5 ICA based method to detect forgery

4.5.1 Proposed work

Consider a simple linear model which consists of N sources of T samples i.e. Si = [Si (1), ...,Si(t),...,Si(T)]. The symbol 't' represents time, but it may represent some other parameter like space. M weighted mixtures of the sources are observed as X, where Xi = [Xi(1),... ,Xi(t),... ,Xi(T)]. This can be represented as: X = A S + n

Where $X=(X_1, X_2, X_3\ldots\ldots\ldots, X_M)$; $S=(S_1, S_2, S_3\ldots., S_N)$ and $n=(n_1, n_2, n_3\ldots\ldots\ldots, n_k)$ where n represent the additive white Gaussian noise (AWGN). It is assumed that there are at least as many observations as sources i.e. M = N. The M × N matrix A is represented as

$$A=\begin{bmatrix} a_{11} & . & . & . & a_{1N} \\ a_{21} & . & . & . & a_{2N} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{M1} & . & . & . & a_{MN} \end{bmatrix}$$

A relates X and S. A is called the mixing matrix. The estimation of the matrix S with knowledge of X is the linear source separation problem. If the additive noise n is negligible, then the original sources can be estimated by evaluating the pseudo inverse of the matrix A, which is known as the un-mixing matrix B, such that BX = BAS = S. For the cases where the number of observations M equals the number of sources N (i.e. M = N), the mixing matrix A

is a square matrix with full rank and $B = A^{-1}$. If there is no prior knowledge of the mixing matrix A, then the estimation of both A and S is known as a blind source separation (BSS) problem. Estimation of the underlying independent sources is the primary objective of the BSS problem.

In the present work Fixed Point ICA [30] is applied on different images. FPICA works on the principle of minimization and maximization of Kurtosis. It converges faster than the other ICA variations. Two forged images are taken as the mixed signals and provided as inputs to FPICA. The estimated independent sources are given as output. The method has been applied to detect copy move attack. ICA can be applied on the parts of the same image to detect the traces of copy move forgery. If two instance of image are copy moved, then ICA will return only one independent estimated source.

4.5.2 Experimental results

The experiment is conducted by creating multiple forged images from same original image. The result of one such instance is shown below.

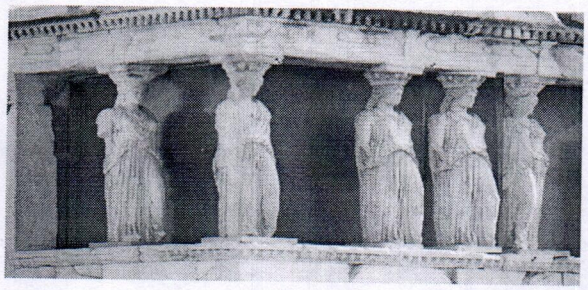


Figure 15(a): First forged image created by copy and pasting one of the statues.

Figure 15(b): Second forged image created by copy pasting one statue at different place

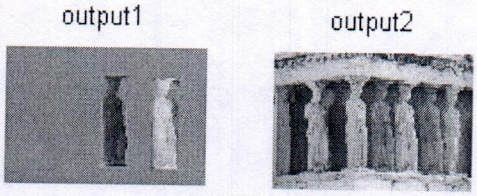


Figure-15(c): Estimated sources by applying blind source separation on the forged images 1(a) and 1(b). Output1 is showing the copy pasted region and output2 showing original image with the locations of pasted region

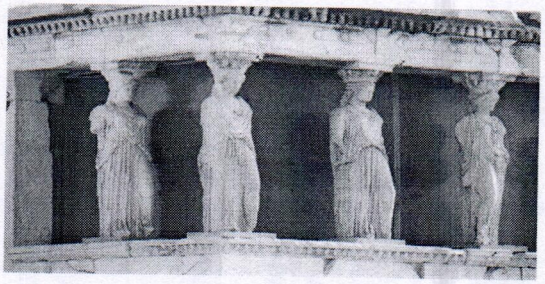


Figure-15(d): Original image having four statues

4.5.3 Conclusion

The results will reflect the importance and application of ICA for blind source separation. In case of more than two instances being presented to the ICA, it will result in the output being independent estimated sources. Even if one of them is original, then also copy moved region is shown as independent component. Also it's evident that ICA is capable to handle the manipulations like scaling and tilting, which is a major limitation in other existing conventional methods. The method is also effective to detect forgery due to splicing of images. To conclude, the proposed work performs well with a small limitation of the two instances should be of equal size.

5. List of Publications

- Sunil Kumar, P.K. Das, S. Mukherjee," Copy-Move Forgery Detection in Digital Images: Progress and Challenges" in *International Journal on Computer Science and Engineering*, volume,3, 2011, pp652-663 ,ISSN:0975-3397 (IC value: 5.08).

- Sunil Kumar, J. Desai, P.K. Das, S. Mukherjee," Suitability of Independent Component Analysis in Digital Image Forgery Detection" in *International Journal of Engineering and Technology*, volume,5,2013,pp226-231 ISSN:0975-4024(Indexed by SCOPUS).

- Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee," Copy Move forgery detection in contrast variant environment using binary DCT vectors", in *International Journal of Image, Graphics and Signal Processing;* Communicated , ISSN:2074-9082(indexed by INSPEC, WorldCat).

- Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee," A fast keypoint based hybrid method for copy move forgery detection", in *International Journal of Computing and Digital Systems*; Communicated , ISSN:2210-142X (indexed by INSPEC)

- Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee," A Fast DCT Based Method for Copy Move Forgery Detection", in *ICIIP-2013*, 2013, pp649-654, ISBN: 978-1-4673-6099-9 (indexed by IEEE Explore, SCOPUS).

- Kumar Sunil, Desai Jagannath, Mukherjee Shaktidev," DCT-PCA Based Method for Copy-Move Forgery Detection", in *Advances in Intelligent Systems and Computing,* Volume 249, 2014, pp 577-583, ISSN: 2194-5357(Indexed by ISI Proceedings, EI-Compendex, DBLP and SCOPUS).

6. References

[1] http://www.fourandsix.com/photo-tampering-history/, "Image Authentication and Forensics | Fourandsix Technologies - Photo Tampering throughout History." .

[2] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Investig.*, vol. 10, no. 3, pp. 226–245, Oct. 2013.

[3] M. Sridevi, C. Mala, and S. Sanyam, "Comparative Study of Image Forgery and Copy-Move Techniques," in *Advances in Computer Science, Engineering & Applications SE - 71*, vol. 166, D. C. Wyld, J. Zizka, and D. Nagamalai, Eds. Springer Berlin Heidelberg, 2012, pp. 715–723.

[4] S. Kumar, P. Das, and S. Mukherjee, "Copy-Move Forgery Detection in Digital Images: Progress and Challenges.," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 2, pp. 652–663, 2011.

[5] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *INDIN '05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.*, 2005, pp. 709–716.

[6] M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-Based Image Forgery Detection: A Review," *IETE J. Educ.*, vol. 55, no. 1, pp. 40–46, Aug. 2014.

[7] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic Sci. Int.*, vol. 171, no. 2, pp. 180–189, Oct. 2007.

[8] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," in *Information Hiding SE - 5*, vol. 6387, no. 8, R. Böhme, P. L. Fong, and R. Safavi-Naini, Eds. Springer Berlin Heidelberg, 2010, pp. 51–65.

[9] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," *Dept. Comput. Sci., Dartmouth Coll. Tech. Rep. TR2004-515*, pp. 1–11, 2004.

[10] G. L. G. Li, Q. W. Q. Wu, D. T. D. Tu, and S. S. S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD," *Multimed. Expo, 2007 IEEE Int. Conf.*, pp. 2007–2010, 2007.

[11] A. Fridrich, B. Soukal, and A. Lukáš, "Detection of copy-move forgery in digital images," *Proc. Digit. Forensic Res. Work.*, 2003.

[12] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," *Syst. Signals Image Process. (IWSSIP), 2011 18th Int. Conf.*, pp. 1–4, 2011.

[13] S. Bayram, H. Taha Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2009, pp. 1053–1056.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," *2008 IEEE Pacific-Asia Work. Comput. Intell. Ind. Appl.*, pp. 272–276, Dec. 2008.

[15] B.L.Shivakumar1 and Lt. Dr. S.Santhosh Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF," *Int. J. Comput. Sci. Issues*, vol. 8, no. 4, pp. 199–205, 2011.

[16] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images.," *Forensic Sci. Int.*, vol. 206, no. 1–3, pp. 178–84, Mar. 2011.

[17] W. Luo and J. Huang, "Robust Detection of Region-Duplication Forgery in Digital Image," *18th Int. Conf. Pattern Recognit.*, pp. 746–749, 2006.

[18] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic Sci. Int.*, vol. 214, no. 1–3, pp. 33–43, 2012.

[19] M. Alsawadi, G. Muhammad, M. Hussain, and G. Bebis, "Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering," *Model. Symp. (EMS), 2013 Eur.*, pp. 249–254, 2013.

[20] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," *Forensic Sci. Int.*, vol. 231, no. 1–3, pp. 61–72, Sep. 2013.

[21] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," *Inf. Sci. (Ny).*, vol. 239, pp. 253–265, Aug. 2013.

[22] X. Pan and S. Lyu, "Detecting image region duplication using SIFT features," *IEEE Int. Conf. onAcoustics Speech Signal Process.*, pp. 1706–1790, 2010.

[23] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, and A. Del Bimbo, "Geometric tampering estimation by means of a sift-based forensic analysis," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2010, pp. 1702–1705.

[24] M. Jaberi, G. Bebis, M. Hussain, G. Muhammad, C. Science, and S. Arabia, "Accurate and robust localization of duplicated region in copy-move image forgery," *Mach. Vis. Appl.*, vol. 25, no. 2, pp. 451–475, 2014.

[25] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD -2014; New database for copy-move forgery detection," *ELMAR, 2013 55th Int. Symp.*, no. September, pp. 49–54, 2013.

[26] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *Inf. Forensics Secur. IEEE Trans.*, vol. 7, no. 6, pp. 1841–1854, Aug. 2012.

[27] W. Chen, M. J. Er, and S. Wu, "PCA and LDA in DCT Domain," *Pattern Recogn. Lett.*, vol. 26, no. 15, pp. 2474–2482, Nov. 2005.

[28] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," *Comput. Vision–ECCV 2006*, 2006.

[29] S. Leutenegger, M. Chli, and R. Y. Siegwart, "BRISK: Binary Robust invariant scalable keypoints," *2011 Int. Conf. Comput. Vis.*, pp. 2548–2555, Nov. 2011.

[30] E. Oja and A. Hyvarinen, "Fast and robust fixed-point algorithms for independent component analysis," *Neural Networks, IEEE Trans.*, vol. 10, no. 3, pp. 626–634, May 1999.